



AI 자율 위협 Mythos 대응 : 차세대 인프라 방어 전략

허재홍 상무

브로드컴 (VMware by Broadcom)



Agenda

1. AI 에이전트 보안 위협과 이에 대응하는 VCF 보안 아키텍처
2. DFW1-2-3-4 마이크로 세그먼테이션 및 가상 패치
3. vDefend 도입 가치
4. Summary



Frontier AI Models: 보안 위협 환경이 근본적으로 변화

April 20, 2026



"Risk of frontier AI is not just a cybersecurity issue, but a resilience issue for global stability"

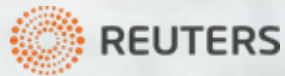
[Web Economic Forum](#)



April 17, 2026

"Time to exploit new vulnerabilities has been reduced from days or weeks to mere hours"

[ISACA](#)



April 13, 2026

Experts warn Mythos could expose legacy banking systems to unprecedented cyber risks

[Reuters](#)



April 7, 2026

"Mythos Preview has identified thousands of zero-day critical vulnerabilities – the oldest found so far is a 27-year old bug in OpenBSD"

[SecurityWeek](#)



AI Mythos의 성능

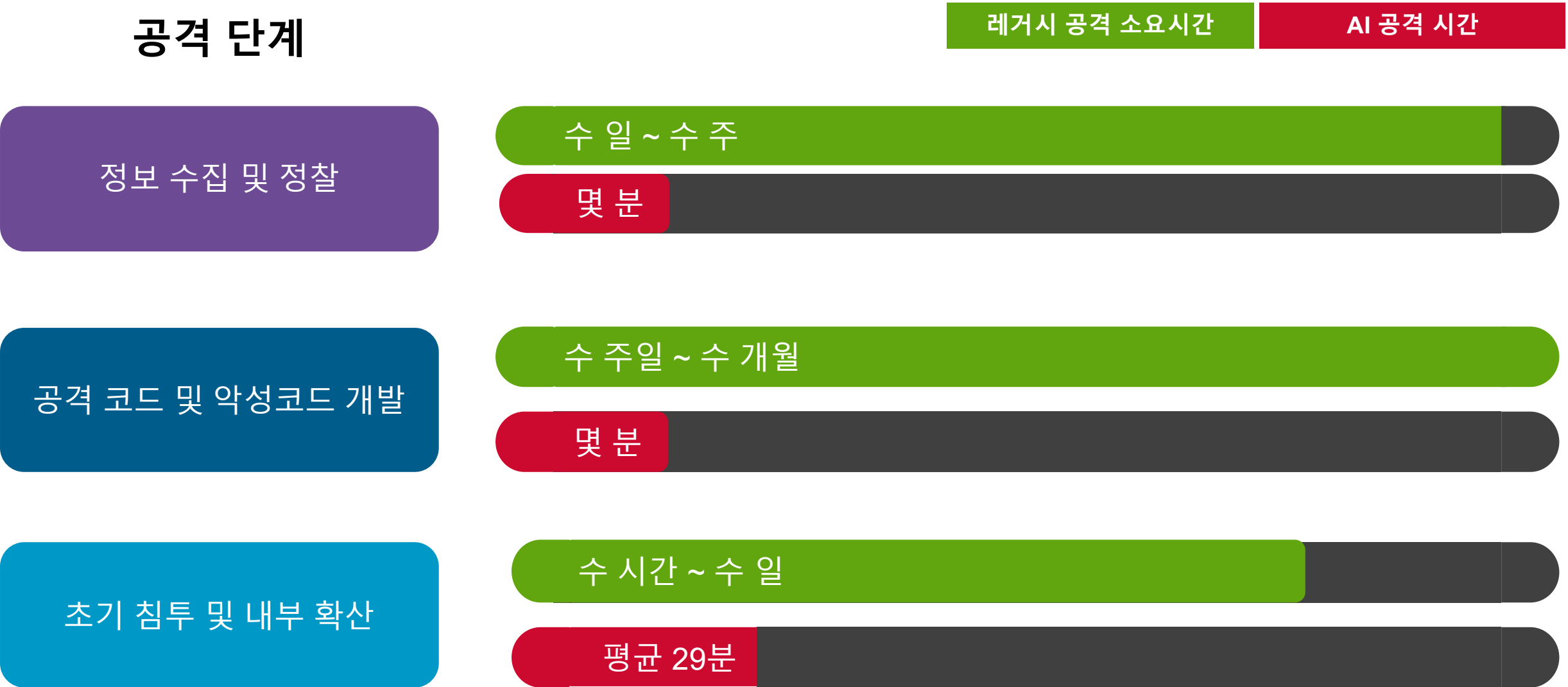
27년 동안 숨겨져 있던 OpenBSD의 제로 데이 취약점 발견

파이어폭스 브라우저를 포함한 핵심 소프트웨어 1만개 이상의 취약점 대량 발굴

고도화된 ‘익스플로잇 체이닝(Exploit Chaining)’과 샌드박스 우회 증명



에이전트 AI 공격과 레거시 공격 시간 비교

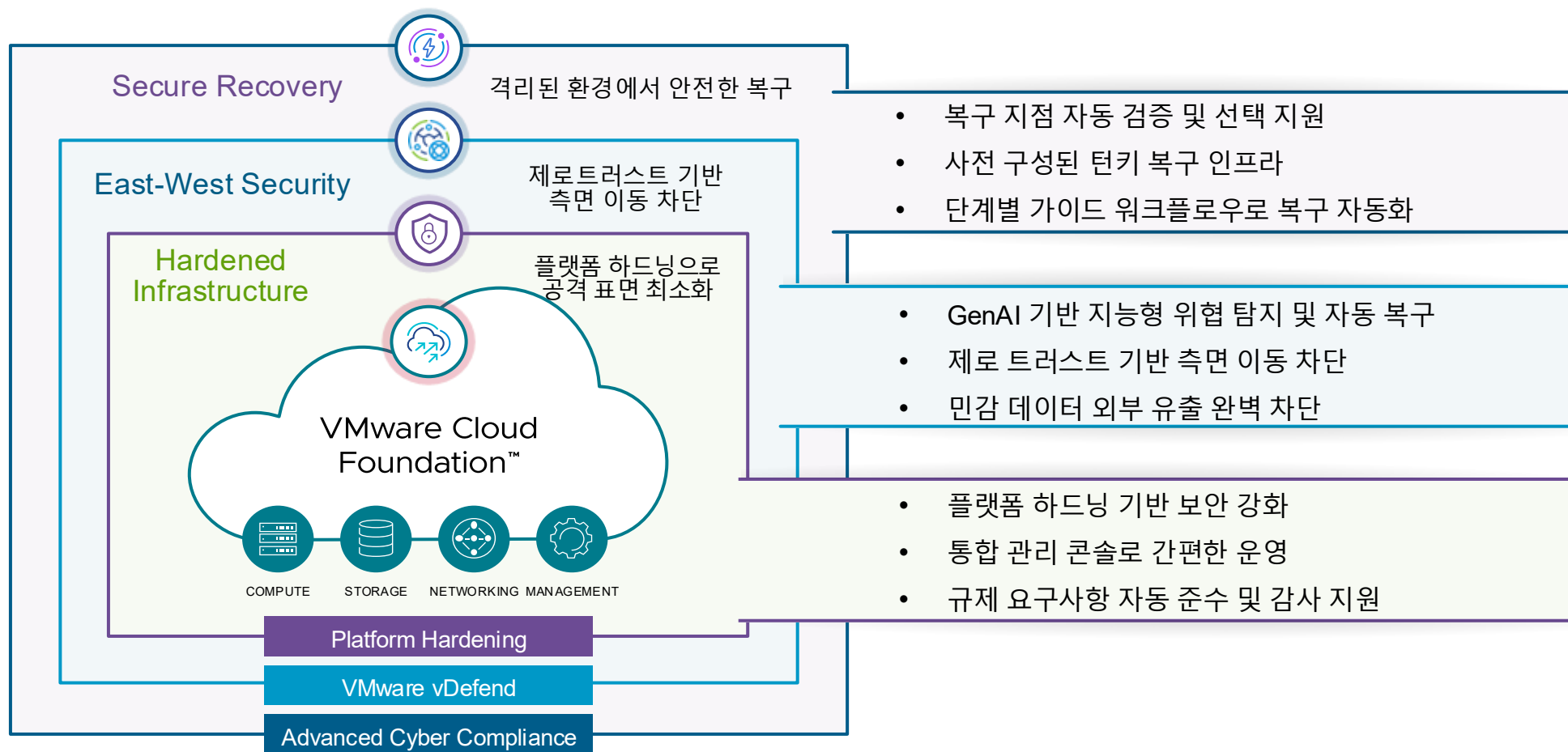


출처: Mandiant, CrowdStrike



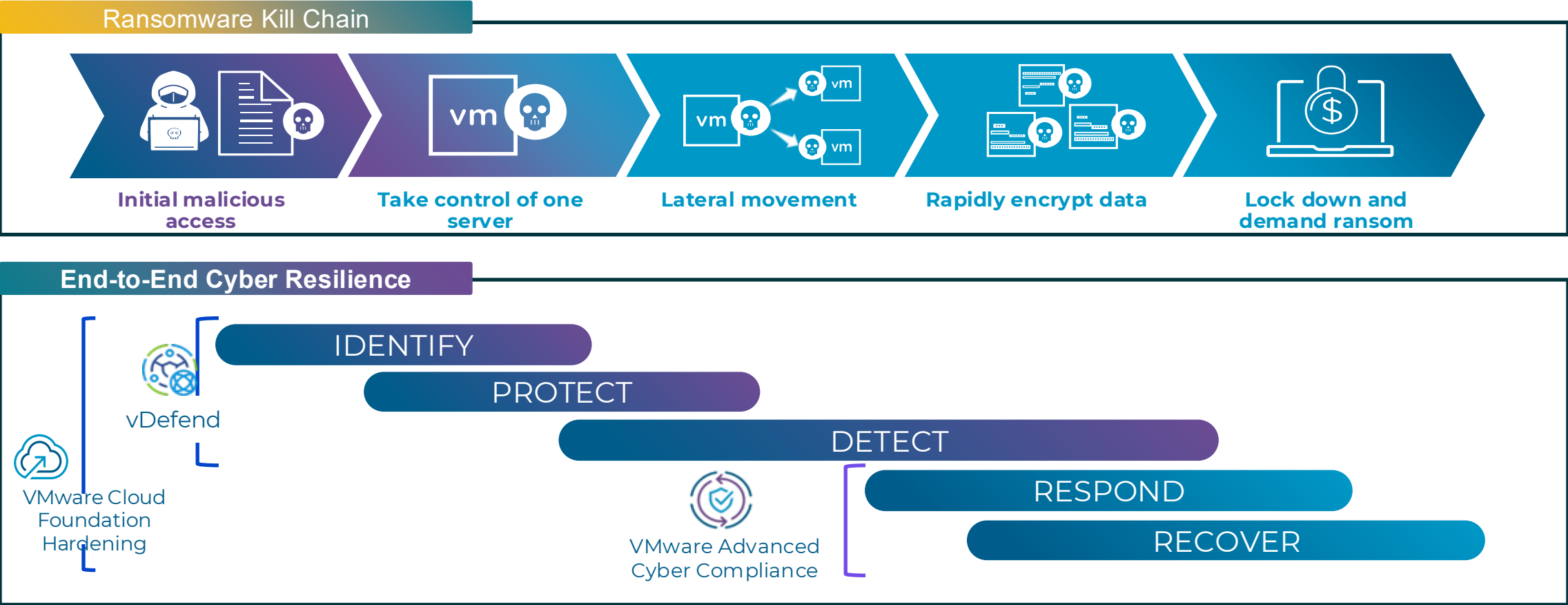
VCF의 포괄적인 내재적 보안 아키텍처

인프라 전반에 보안을 내재화 하여 공격 표면을 원천 차단하고, 사고 발생 시에도 비즈니스 연속성을 즉시 복원

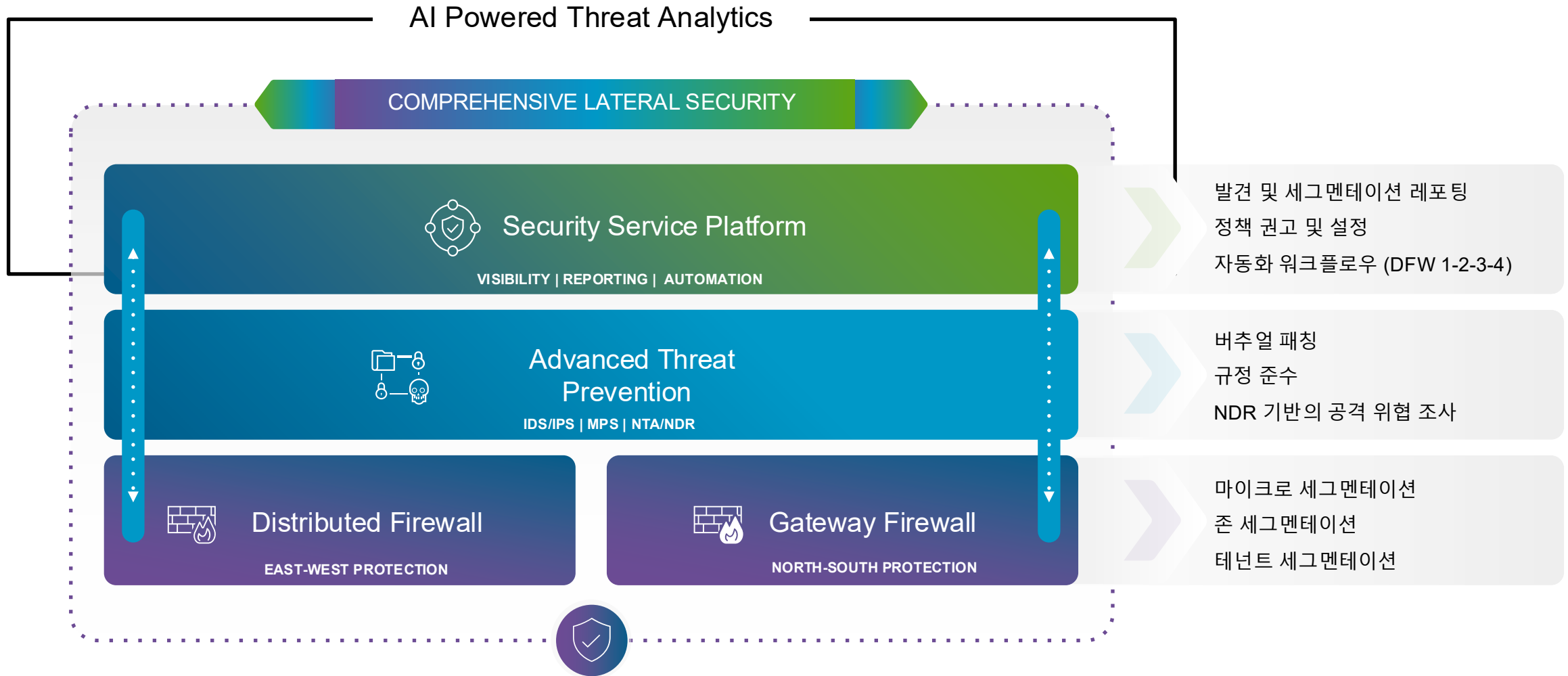


사이버 킬 체인 방어 프레임워크 기반의 VCF 보안 플랫폼

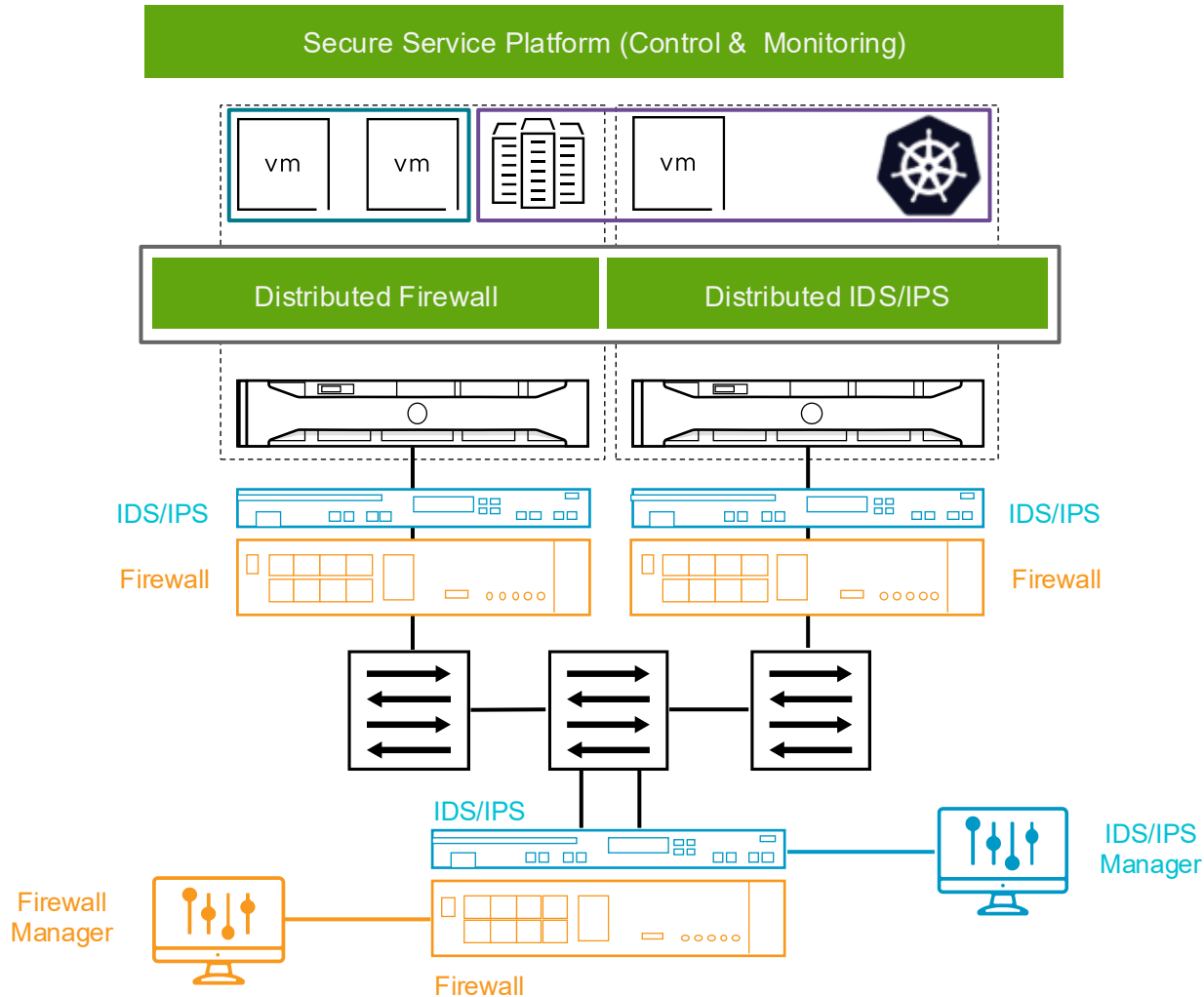
VCF 통합 보안 플랫폼은 킬체인 전 단계에서 위협을 차단하며, 탐지부터 복구까지 단일 플랫폼 내에서 자동화된 보안 루프를 완성합니다. 지능형 차단으로 확산을 봉쇄하고, 자동화된 클린룸 복구로 비즈니스 연속성을 실현합니다



vDefend 솔루션의 구성요소



vDefend 솔루션의 구성 및 특징



- 인-커널 기반으로 동작하기 때문에 트래픽 병목현상을 최소화
- 태그 기반으로 오브젝트를 분리하여 동적이고, 효율적인 트래픽 제어
- 탭-리스 기반의 실시간 트래픽 모니터링
- MI/ML 프로세스를 통한 보안 정책 생성 및 권고

vDefend와 Avi - VCF 및 AI 워크로드를 위한 최고의 보안솔루션

Cybersecurity Recommendations

엔드 포인트 중심의 보안 체계(EDR)를 네트워크 제어 영역까지 확장하여 감시하고 통제



제로 트러스트 네트워크 세그먼테이션



행위 분석을 통한 능동적인 보안 모델



신속한 패치 워크플로우



vDefend + Avi: Multi-layer Cybersecurity

vDefend와 Avi를 기반으로 하는
멀티 레이어 프라이빗 클라우드

vDefend Distributed Firewall (DFW) 기반
제로트러스트 네트워크

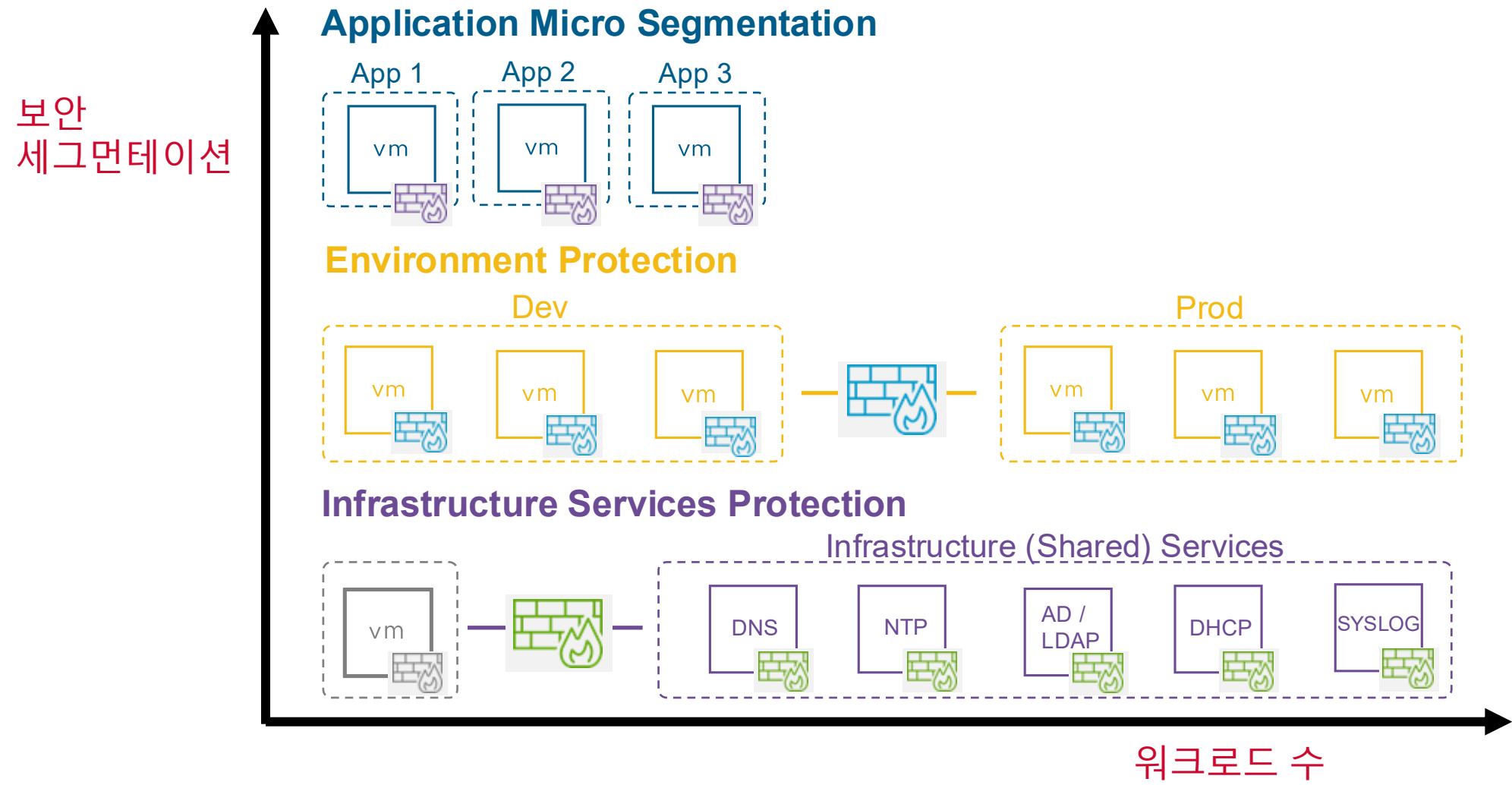
vDefend NTA/NDR

가상 패칭: vDefend IDPS & Avi WAF



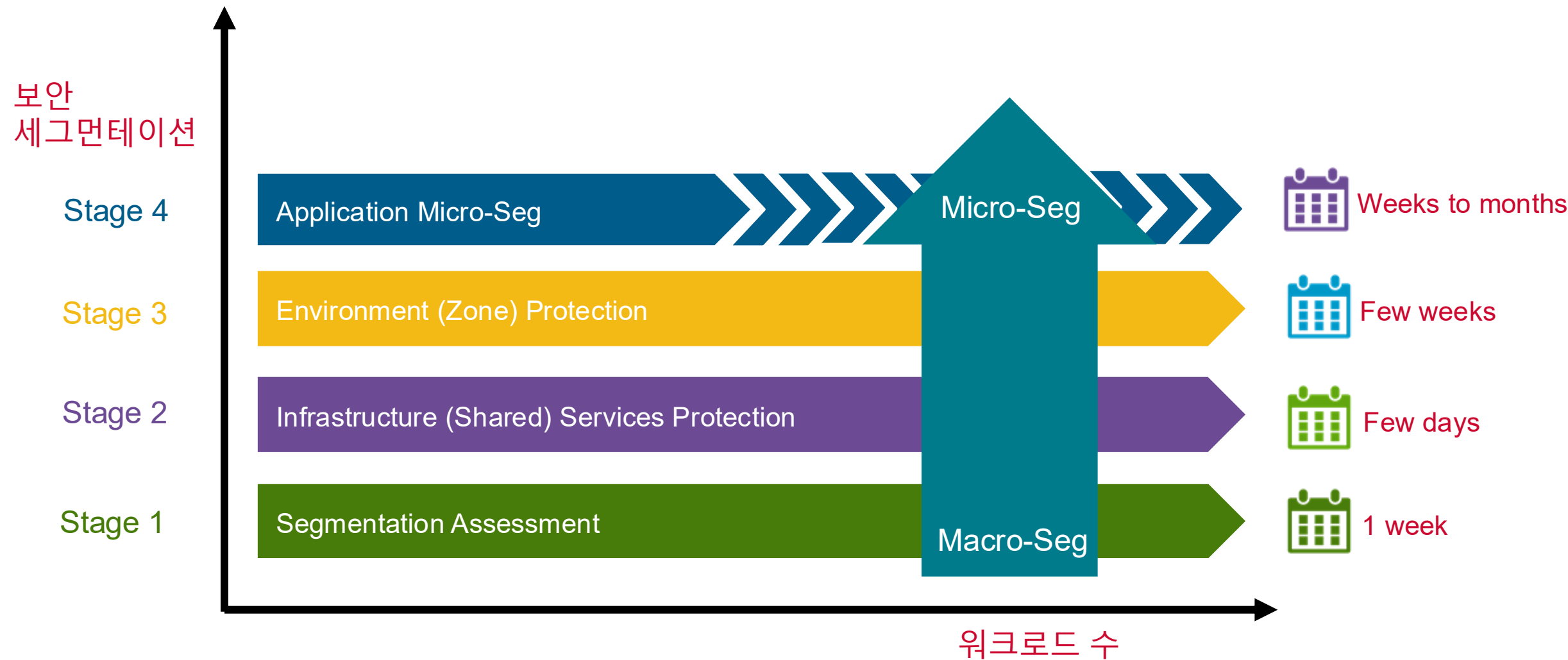
워크플로우를 기반으로 마이크로 세그멘테이션을 구축

DFW 1-2-3-4



자동화 워크플로우 기반의 마이크로 세그먼테이션 환경을 구성

DFW 1-2-3-4



Stage 1: 실시간 트래픽을 바탕으로 인프라 보안 상태를 측정

vDefend Console



* Considers all discovered workloads minus Infrastructure.
** Based on Security Services Platform Applications (a special group). Critical application type is weighted higher.

Score Factor	Score Factor Progress	Current Score
Distributed Firewall In Operation Security Feature Activation	 Score Breakdown 2.5/2.5 Stateful Distributed Firewall Activated 2.5/2.5 Malicious IP Protection Activated	5 /5
Infrastructure Protection Percentage of protected Infrastructure traffic		0 /5
Environment Protection Percentage of all compute covered by at least one environment rule and number of environment pairs in Blocked mode.	 Score Details 0/2.5 Percentage of Environment Pairs in Blocked mode 0/2.5 Percentage Of All Computes Covered By At Least One Environment Rule *	0 /5
Application Workload Protection Percentage of protected workload, their criticality, traffic and presence of deny rules.	 Score Breakdown 0/10 Application Workload Coverage 0/25 Application Lock-Down** 0/10 Application Traffic Coverage 0/25 Data Center Lock-Down	0 /70
Workloads without Obsolete OS & Risky Protocols Percentage of workload not at risk of obsolete OS nor allowing connections via risky protocols.		4.2 /10

Stage-1: Segmentation Assessment & Report

- *SSP 기반 모델
- 수행 기간: 1주

Security Journey

☒ Show Journey Status on Homepage

- 실시간 트래픽 수집으로 분석된 인프라 보안 평가 점수

vDefend Security Journey Starts Here!

The Security Journey prescribes a multi-stage segmentation workflow to speed up zero trust implementation with VMware vDefend Distributed Firewall. Continuous monitoring at each stage highlights any deviations and allows recalibration of security posture.

Instruction: Track progress by clicking the stage indicator ○ to mark it "Reviewed".



No Existing Score Available

[CALCULATE SCORE](#)

0 out of 4 stages reviewed



STAGE 1

Assess Segmentation Posture



STAGE 2

Secure Infrastructure Shared Services



STAGE 3

Create and Secure Environments



STAGE 4

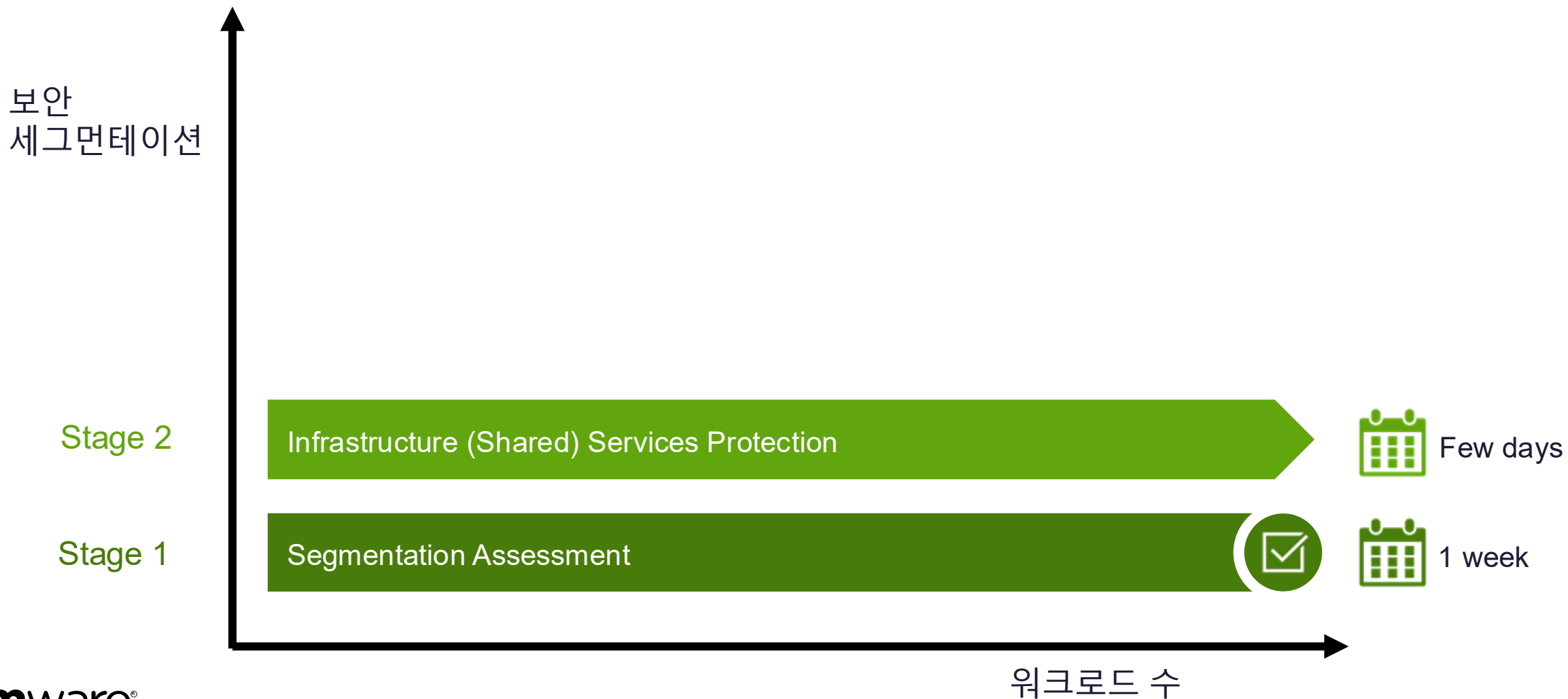
Micro-Segment Applications



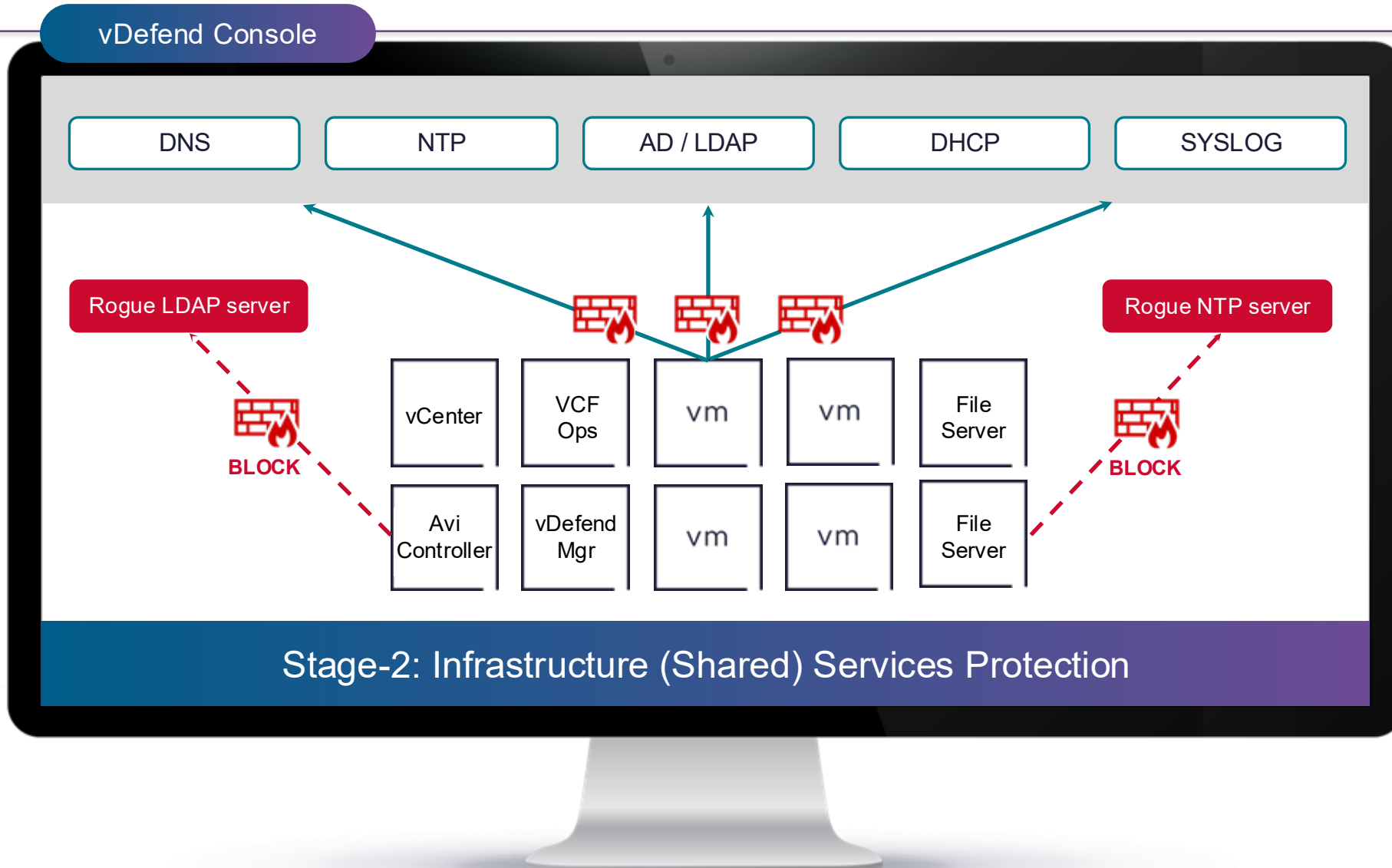
Refer to the Appendix A for a detailed explanation of the Security Segmentation Scoring methodology. Subsequent chapters of this report offer an in-depth analysis for workload categories, their traffic and related risks along with a set of recommended best practices for implementation.

36711 At-Risk Entry Points	At-risk Workloads that can potentially act as entry points for lateral movement in the data center.
1/1 At-Risk Communication Chains	Communication chains with at least one at-risk workload having some unprotected traffic.
66078/66078 Workloads Within Blast Radius	Workloads part of an at-risk communication chain that could become target of lateral movement because of unprotected traffic.
2.17M/2.18M Unprotected Unique Flows	Number of unprotected data flows hitting default allow rule.

모든 애플리케이션을 위한 측면 보안 – 신속한 배포 여정



Stage 2: 공통 인프라 서비스 식별 및 보안정책 수립



Few days

Segmentation Monitoring

[GO TO SEGMENTATION PLANNING](#) ⓘ

Infrastructure Services

Environments

Applications

Summary



Last 7 Days ▾

1 / 14 SERVICES AVAILABLE FOR UPDATE

New Detected Servers

10

[UPDATE INFRASTRUCTURE ASSETS](#)

SECURITY RULES

No Recommended Rules ⓘ

8 Services

Missing Some Recommended Rules ⓘ

0 Services

With All Recommended Rules ⓘ

5 Services

[REVIEW & ADD RULES](#)

Auto-Discovered

Infrastructure Service	Infrastructure Asset
> DNS-UDP	DNS-UDP_Group
> LDAP	LDAP_Group
> Syslog	Syslog_Group
> NTP	NTP_Group

Untrusted

New Detected Servers ⓘ

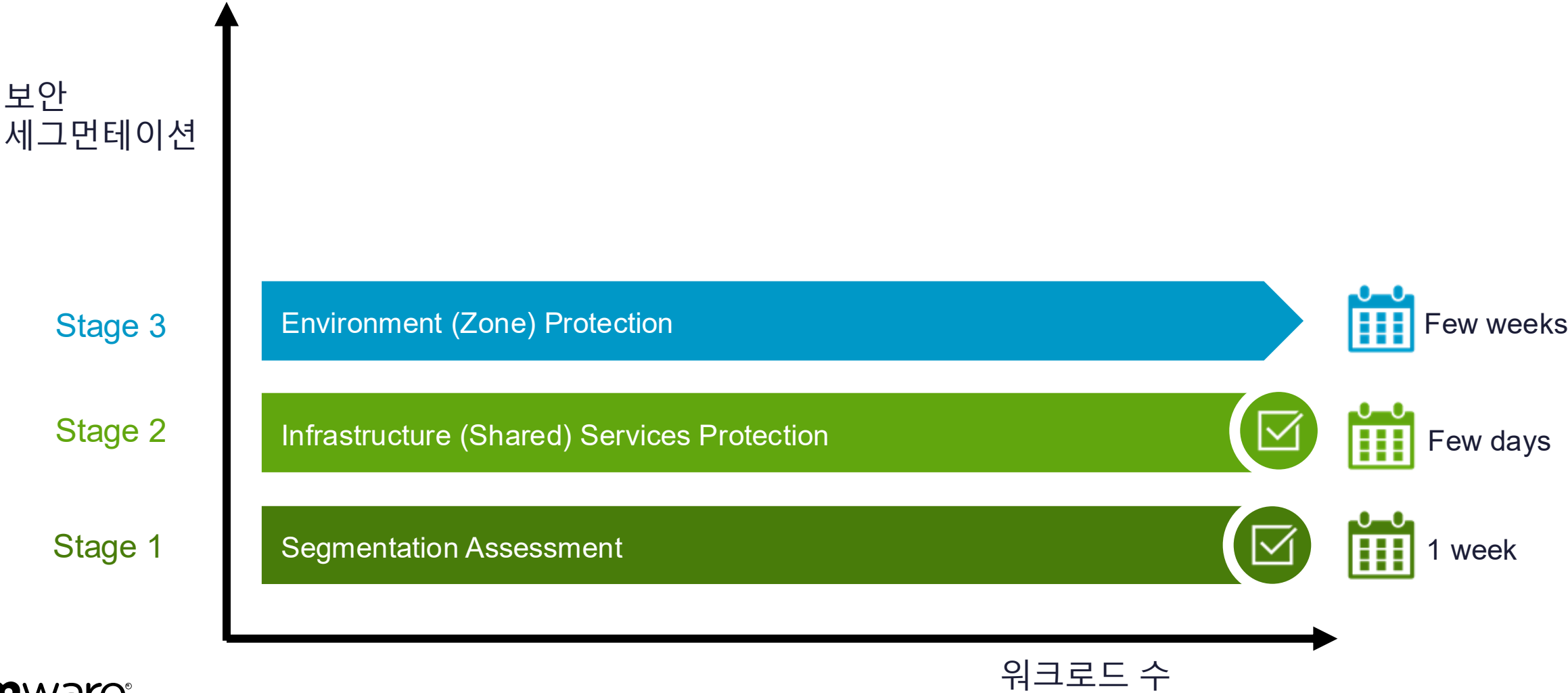
10

Recommendations

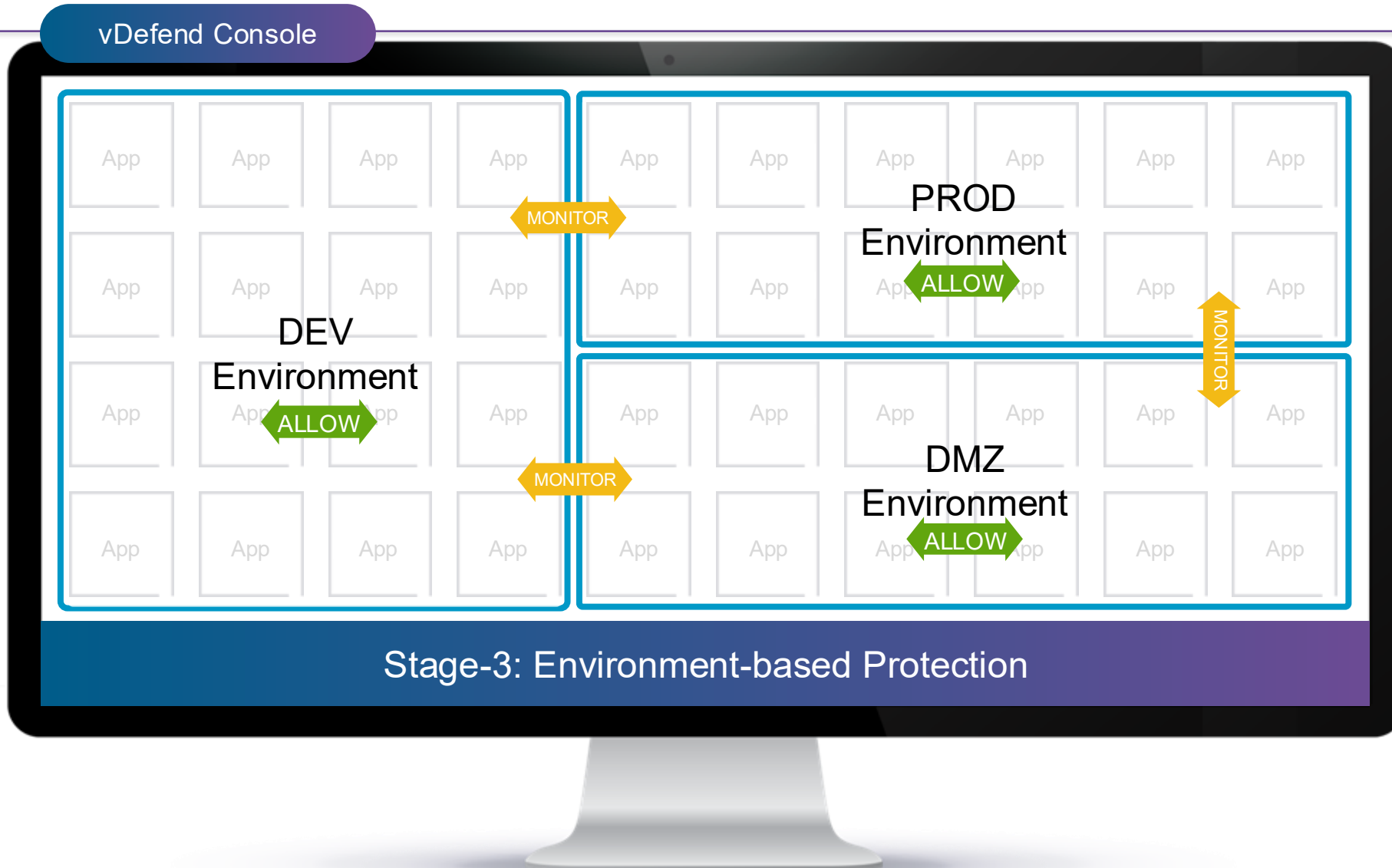
Security Rules

Traffic Rule	Lockdown Rule	View	ACTION ▾
Traffic Rule	Lockdown Rule	View	ACTION ▾
Traffic Rule	Lockdown Rule	View	ACTION ▾
Traffic Rule	Lockdown Rule	View	ACTION ▾

모든 애플리케이션을 위한 측면 보안 – 신속한 배포 여정

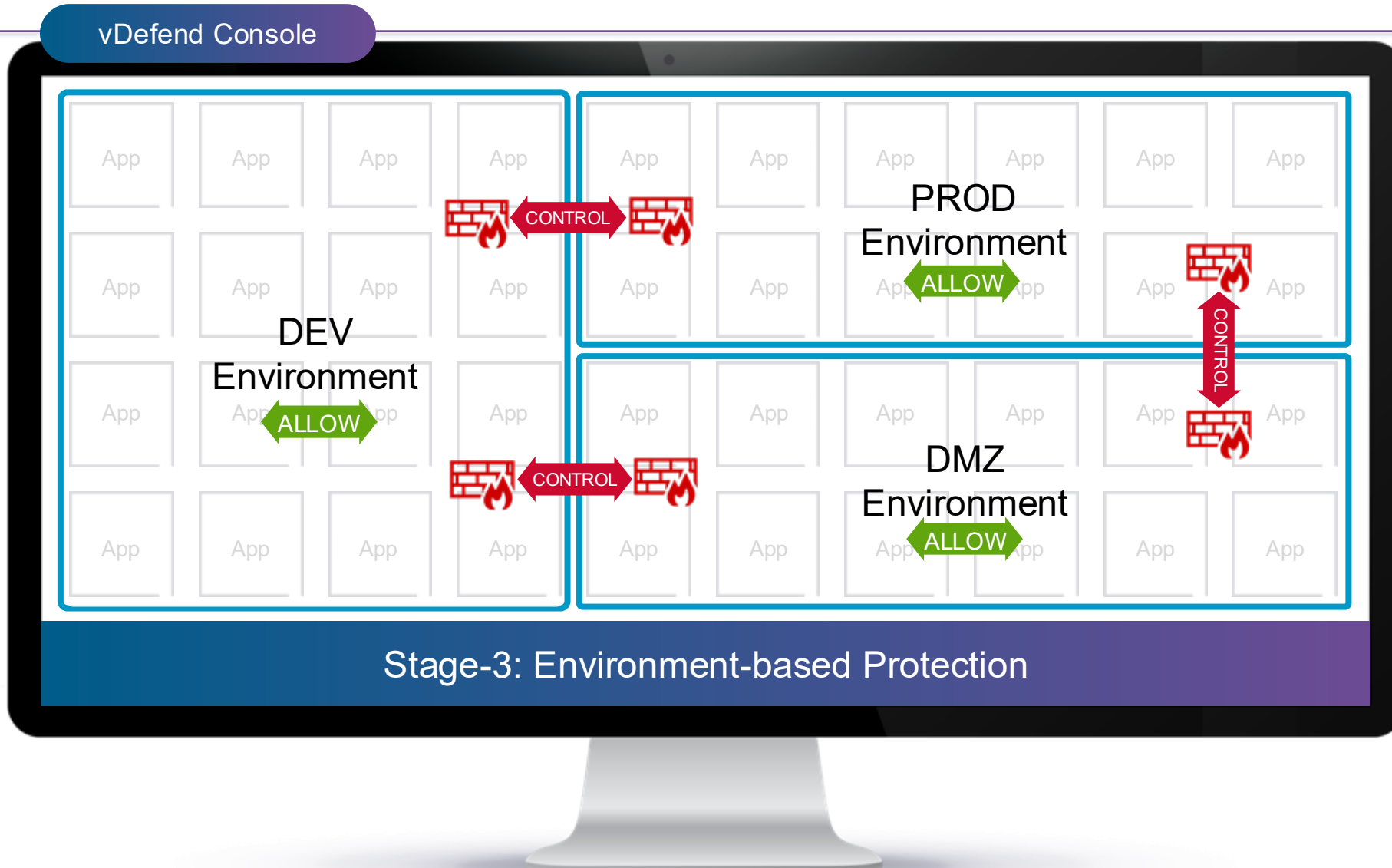


Stage 3: 환경 수준의 보호를 통한 공격 표면 축소



Few weeks

Stage 3: 환경 수준의 보호를 통한 공격 표면 축소



Few weeks



Monitor & Plan Overview

Security Posture

Security Explorer

Segmentation Monitoring

Network Detection & Response

Threat Monitoring

Firewall Insights

Infrastructure Services

Environments

Applications

Publishing or starting discovery of recommendation(s) for inter-environment pairs. The process can take some time. Check later to view the updates; a page refresh may be needed.

Select Environments

prod X

dev X

2 out of 2 environments selected. [Reset to Default](#)

SUMMARY FOR SELECTED ENVIRONMENTS

ENVIRONMENTS COUNT

Environments

Environment Pairs

2

2

PROTECTION RULE ACTION SUMMARY

Block

Allow

Jump-to Application

No Protection Rule

0

0

0

2

DETAILS

Without Inter-Environments Policy & Rules

2

2 Pairs governed by Environment Category Default Rule

prod To dev



Protection Rule Action

No Protection Rule

[Go Edit Rule Action](#) 

Inter-Environment Policy & Rules

None



Inter-Environment Traffic Detected

Yes (2 flows)

[Go To Environment Monitoring](#)[View Traffic in Security Explorer](#)[Run Recommendation](#)Prod $\longleftrightarrow$ Dev 보안 정책 미적용 중



Monitor & Plan Overview

Security Posture

Security Explorer

Segmentation Monitoring

Network Detection & Response

Threat Monitoring

Firewall Insights

Infrastructure Services

Environments

Applications

🔔 Publishing or starting discovery of recommendation(s) for inter-environment pairs. The process can take some time. Check later to view the updates; a page refresh may be needed.

Select Environments ⓘ

prod X

dev X

2 out of 2 environments selected. [Reset to Default](#) ⓘ

SUMMARY FOR SELECTED ENVIRONMENTS

ENVIRONMENTS COUNT

Environments

Environment Pairs

2

2

PROTECTION RULE ACTION SUMMARY

Block

Allow

Jump-to Application

No Protection Rule

0

0

0

2

DETAILS

Without Inter-Environments Policy & Rules

2

2 Pairs governed by Environment Category Default Rule

prod To dev



- Protection Rule Action No Protection Rule [Go Edit Rule Action](#) ⓘ
- Inter-Environment Policy & Rules None
- Inter-Environment Traffic Detected Yes (2 flows)

[Go To Environment Monitoring](#) | [View Traffic in Security Explorer](#)[Run Recommendation](#)

보안 정책 생성 및 권고

Block
Prod ↔ Dev



Monitor & Plan Overview

Security Posture

Security Explorer

Segmentation Monitoring

Network Detection & Response

Threat Monitoring

Firewall Insights

Infrastructure Services

Environments

Applications

❗ Publishing or starting discovery of recommendation(s) for inter-environment pairs. The process can take some time. Check later to view the updates; a page refresh may be needed.

Select Environments ⓘ

prod X dev X

2 out of 2 environments selected. [Reset to Default](#) ⓘ

SUMMARY FOR SELECTED ENVIRONMENTS

ENVIRONMENTS COUNT

Environments

Environment Pairs

2

2

PROTECTION RULE ACTION SUMMARY

Block

Allow

Jump-to Application

No Protection Rule

2

0

0

0

DETAILS

Without Inter-Environments Policy & Rules

0

0

Pairs governed by Environment Category Default Rule

Destination		
Source	dev	prod
dev		
prod		

두 개의 환경간 트래픽은
신규 정책으로 모두 제어
BLOCKED

Overview

Security Intelligence

Security Explorer

Segmentation Planning

Segmentation Monitoring

Policy Recommendations

Threat Monitoring

Network Detection & Res...

Malware Prevention

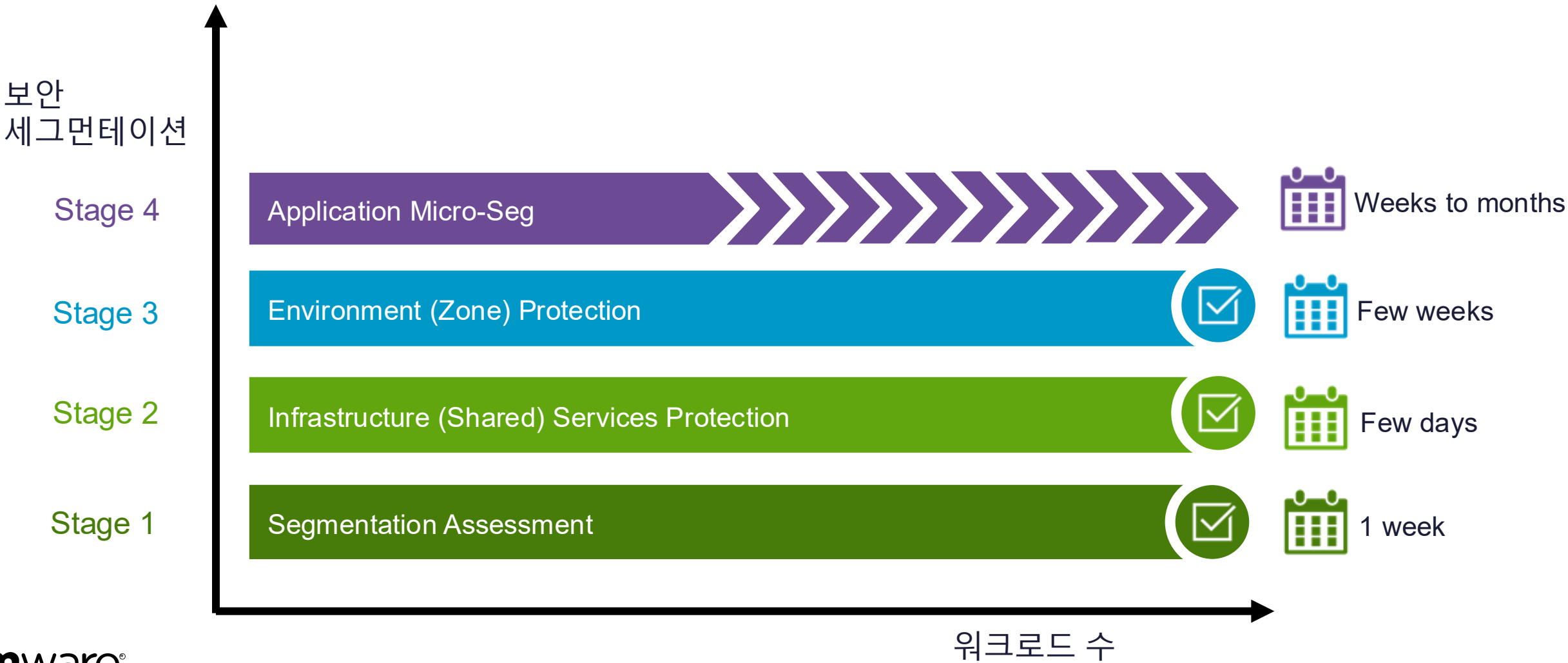
Suspicious Traffic

Reports

Security Segmentation R...

Flow Export

모든 애플리케이션을 위한 측면 보안 – 신속한 배포 여정



Stage 4: 애플리케이션 레벨 보호

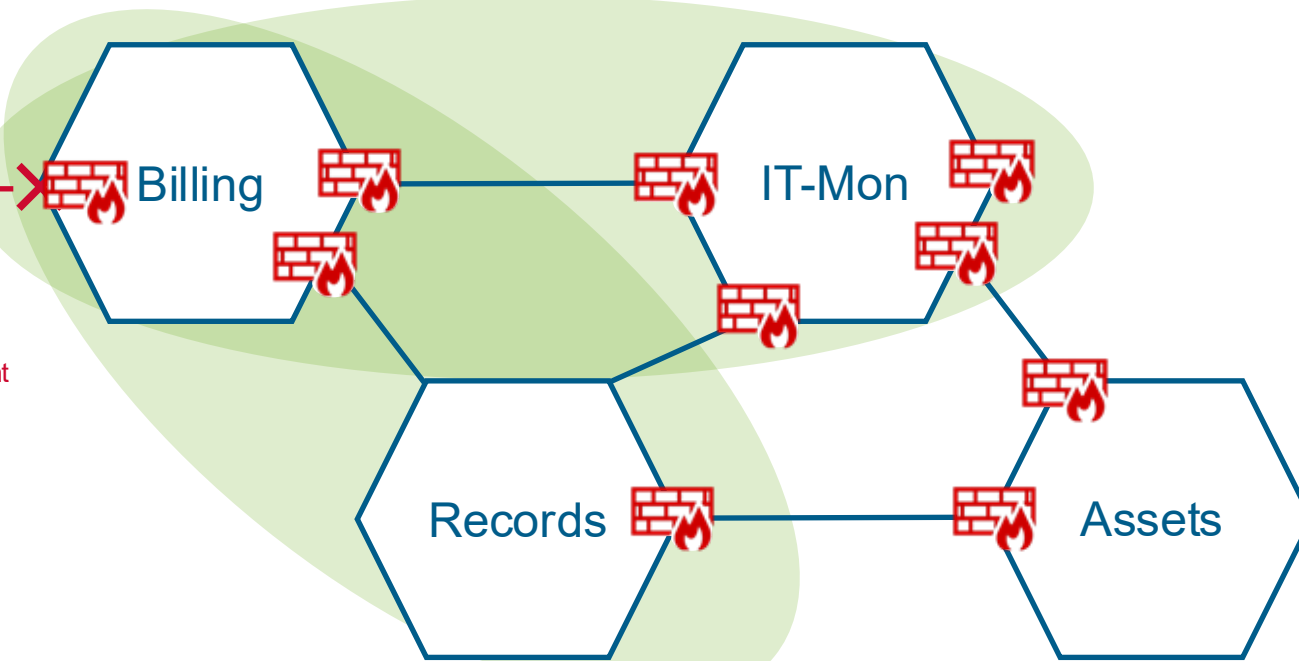


Stage 4: 애플리케이션 레벨 보호

vDefend Console



BLOCK
unauthorized
lateral movement



Weeks to months

Stage-4: App-level Protection

Security Explorer

Security Explorer Preferences

COMPUTES ALL

CLEAR

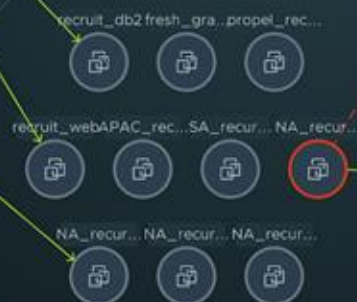
Flows: ☒ Unprotected ☒ Blocked ☒ Allowed

LAST 30 DAYS

Billing (6)



Records (10)



IT Monitoring (7)



Overview

- 어플리케이션 간의 실시간 트래픽 플로우
- 색깔 별로 플로우 상태 확인 (녹색: 제어, 빨간색: 비제어, 파란색: 제어(블락))

Security Journey

☒ Show Journey Status on Homepage

- 워크플로우 완료 시, 최종 보안 평가 및 점수 개선 내역 확인

vDefend Security Journey Starts Here!

The Security Journey prescribes a multi-stage segmentation workflow to speed up zero trust implementation with VMware vDefend Distributed Firewall. Continuous monitoring at each stage highlights any deviations and allows recalibration of security posture.

Instruction: Track progress by clicking the stage indicator ○ to mark it "Reviewed".



Last calculated on 11/12/2025 10:12 am PST



1 out of 4 stages reviewed

- 

STAGE 1 Assess Segmentation Posture

>
- 

STAGE 2 Secure Infrastructure Shared Services

>
- 

STAGE 3 Create and Secure Environments

>
- 

STAGE 4 Micro-Segment Applications

>

분산형 가상 패치 기반의 초고속 방어 체계

전형적인
패치
매니지먼트

Patch
Available

Customer
패치 테스트
(days)

Customer
패치 롤 아웃
(고객사 환경에 따라 수 일 ~ 몇 달까지 소요)

취약점 해결

애플리케이션이 공격에 노출 됨 (days / weeks / months)

가상
패치

Signature
Available

애플리케이션은 가상화 패치로 보호됨 (수 분 ~ 수 시간)

취약점 해결

분산 가상 패치 – VCF 워크로드



vDefend IDPS

ESXi Hypervisor

vDefend IDPS & Avi WAF 분산형 가상 패치: 장점

- 공식 보안 패치가 적용되기 전까지 선제적으로 방어 조치를 통한 보안 위협 최소화
- VM, Container 모두 보호
- 기술지원이 종료된 OS (패치 불가능 OS) 보호
- Custom signature 지원
- 분산형 확장 아키텍처 기반으로 TCO 절약

IDS Signatures

The IDS Signature portal allows you to access detailed information on the IDS/IPS signatures available on the vDefend platform. You can view the details of a specific signature, determine changes across signature bundle versions, export a filtered list, and more.

Bundle Versions: IDSSignatures_3781



Available Bundle Versions: 11 VIEW CHANGE HISTORY

Total Signatures ⓘ

19338



EXPORT CVE(s): CVE-2026-... ⓘ Type or apply filter CLEAR

Signature ID	IDS Severity	Details	Product Affected	Attack Target	Attack Type	CVSS	CVE(s)	Action
1148878	Medium	NSX - (Initial Access) Detect CVE-2026-21858 exploitation attempts	NONE	Web_Server	attempted-user	10	CVE-2026-21858	Reject
2066448	High	ET WEB_SPECIFIC_APPS Node.js n8n Authenticated Workflow Expression Injection (CVE-2025-68613)	Node_js	Server	web-application-attack	10	CVE-2025-68613	Reject

ADD PROFILE

Filter by Name, Path and more

	Name	Description	Tags	Where Used	Status
⋮ >	DefaultIDSProfile		0	Where Used	Success ↻
⋮ v	Virtual Patch: CVE-2026-21858 and CVE-2025-68613		0	Where Used	Success ↻
IDS Signatures					
Manage System and Custom signatures by qualifying filters					
System Included: 2 Total: 19360					
- High - Medium - Suspicious - Critical - Low					
v Additional Options					
Attack Types		0	CVSS	0	
Attack Targets		0	CVEs	2	
Customized actions and/or excluded signatures specific to this profile.					
0					
Note: The available list of customized intrusion signatures is based upon the selected attributes above.					
Manage signatures by Signature IDs					
Packet Capture On					
Packet Capture File Size		10000 Bytes	Total Packets	5	

적용하는 CVE를 기반으로 IDS/IPS
프로파일 생성

IDS/IPS

Monitoring

Packet Capture Query

↗️

❓

↻ REFRESH

INTRUSION ATTEMPTS

Total: 2 24 Hours: 2 ⓘ

Standalone hosts: Off Clusters: 1/2 Gateways: 1/2 Last 24 Hours Timeline

Unique Intrusions (1)

Traffic: ALL TRAFFIC ▼ VIEWING SIGNATURE ACTIONS (3/3) ▼

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 0 SUSPICIOUS 0

Filter by Attack Type or more

Impact Score ⓘ	Severity	Last Detected	ID & Details	Users Affected	Where Detected	CVE Details	CVSS
45	Medium	May 28, 2026, 7:48:55 AM Multiple Attempts	1148878 NSX - (Initial Access) Detec...	1		CVE-2026-21858	10 Critical

Intrusion Event Details (latest occurrence)

Source | ATTACKER

IP: 192.168.100.15 Port: 57982

Destination | TARGET

ubuntu-vulhub IP: 192.168.100.10 Port: 5678

Attack Target	Web_Server	Service	HTTP
Attack Type	attempted-user	Signature ID	1148878
Rx into Attacker	1.06 KB	Signature Revision	33212
Product Affected	View Details	Mitre Tactic	Initial Access
Total Events	2	Mitre Technique	Exploit Public-Facing Application

Intrusion Activity

Prevented Events

May 28, 2026

Number of Attempts: 2

Timeline

May 13 May 15 May 17 May 19 May 21 May 23 May 25 May 27 May 29

가상 패치를 통해서 해당 CVE가 정상적으로 통제되는 것을 모니터링

Prevented Events
May 28, 2026
Number of Attempts: 2

Avi 웹 방화벽

Regularly updated CRS

정기적인 시스템 업데이트
프로토콜 적합성, OWASP
Top-10

예: SQL injection, XSS etc

Positive Security Model

웹 방화벽이 정상적인 패턴을
자가 학습하여, 정상 패턴
이외의 패턴들을 자동으로
차단하는 방식

예: 10 수 패턴 필드

Allowed: 1234567890

Flagged: l23456789O

Critical CVE Specific Signatures

치명적인 신규 CVE 발견 시,
즉각적인 대응 차원에서
회사에서 제공하는 CVE 패치

예: React2Shell

Custom Signatures

고객사 애플리케이션 특성에
맞게 정규식을 사용한 고객
맞춤 패턴 생성 및 제공

예: 어플리케이션이 고객
환경에 맞게 특수하게 개발된
경우

선제적 대응

위협 대응

vDefend 도입 가치

VMware vDefend Software Stack (Single License)

Network Detection & Response

Malware Prevention

Distributed IDS/IPS

Gateway Firewall

Distributed Firewall

Security Intelligence
(Analytics & Recommendations)

Advanced Threat Prevention (ATP)

- Prevent
- Detect
- Remediate

Firewall

- East-west
Visibility
- Zone & Micro-
Segmentation

Lower TCO*

Up to
50% 하드웨어 비용
대비
절감효과*

25% 운영비용
절감*

Better Security*

77% 심층적인
트래픽 보안
(100% East-West)

40% 위협 감소

45% 빠른 배포

*Based on actual customer interviews conducted by third parties or customer examples



Summary

01

인프라 보안 태세 점검 – "SSP Security Assessment"

02

마이크로 세그멘테이션 아키텍처 수립 – "DFW 1-2-3-4 워크플로우"

03

보안 다운타임 없는 긴급한 대응 – "Avi WAF & vDefend IDPS 가상 패치"





Thanks